SDES Example

Ques Generate 2 keys of SDES using Key Generation algorithm & using that sub key encrypt the following data.

Let the plaintext be the string 01110010
Let the 10-bit key be 1010000010.
(only S boxes - S0 & S1 will be given)

solution

$\Rightarrow$ Key = $\overset{1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10}{1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0}$

Step-1

P10.

3	5	2	7	4	10	1	9	8	6

Ans step1 → 1 0 0 0 0 0 1 1 0 0

step-2 left shift by 1

1 0 0 0 0	0 1 1 0 0
left shift by 1	LS-1

Ans step2 → 00001 11000

$\overset{1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10}{0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0}$ → Give this input to step-4

only for K_1

step-3 P8

6	3	7	4	8	5	10	9
1	0	1	0	0	1	0	0

key-1 10100100

Step-4 take input from step-2

input - 0000111000

LS-2	LS-2
00100	00011

1 2 3 4 5 6 7 8 9 10
00100 00011

Step-5

P8

6	3	7	4	8	5	10	9
0	1	0	0	0	0	1	1

key 2 ←

key-1	10100100
key-2	01000011

Encryption

plaintext - 01110010
1 2 3 4 5 6 7 8

Step-1 IP.

2	6	3	1	4	8	5	7
1	0	1	0	1	0	0	1

L R

Step-2 Function.

$f_k(L, R) = (L \oplus F(R, SK), R)$

(i) $F(R, SK) = F(\underset{1\,2\,3\,4}{1001}, SK)$

(i) E/P

4	1	2	3	2	3	4	1
1	0	0	0	0	0	1	1

$\oplus \quad K_1 = 11000011 \quad \oplus \quad 10100100$

$$\begin{array}{r} 11000011 \\ \oplus\ 10100100 \\ \hline 01100111 \end{array}$$

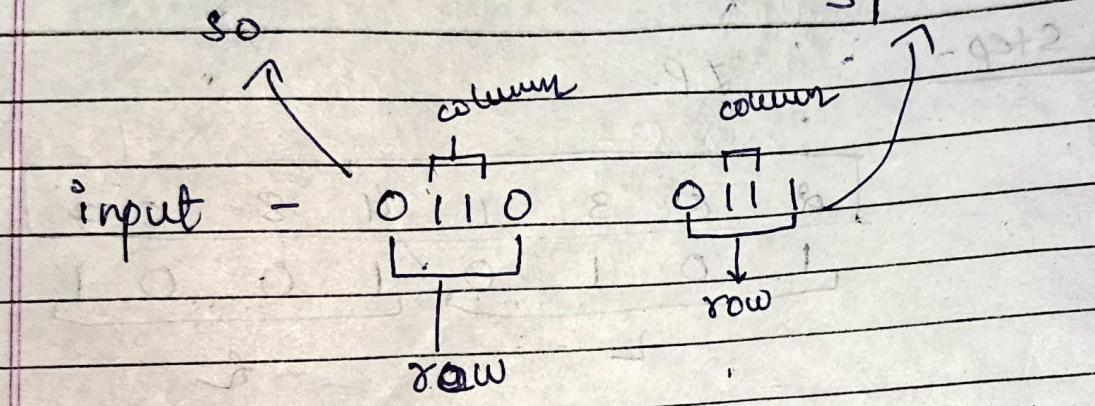
↓ Give it to S_0 ↓ Give it to S_1

	0	1	2	3
0	1	0	3	0
1	3	2	1	0
2	0	2	1	3
3	3	1	0	2

S_0

	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	2
3	2	1	0	3

S_1



$S_0 \rightarrow$ row = 0
column = 3
↓
output = 0
00

$S_1 \rightarrow$ row = 1
column = 3
↓
output = 3
11

↓
0011
1 2 3 4

permutation P4

2	4	3	1
0	1	1	0

So $F(R_1, S_k) = 0110$

$$f_K(L, R) = L \oplus f(R, SK), R$$

$$= 1010 \oplus 0110, 1001$$

$$= 11001001$$

Step - 3 Switch function

$$\underbrace{1001}_{L}\underbrace{1100}_{R}$$

Step - 4 $f_K(L, R) = L \oplus F(R, SK), R)$

$$f(R, K_2) = F(\underset{1\,2\,3\,4}{1100}, K_2)$$

(i) E/P.

4	1	2	3	2	3	4	1
0	1	1	0	1	0	0	1

$01101001 \oplus K_2$

$$\begin{array}{r} 01101001 \\ \oplus\ 01000011 \\ \hline 00101010 \end{array}$$

Give it S_0 S_1

S_0 S_1

S_0 row = 0 row = 2

column = 1 Column = 1

0 0

$f(R, SK) = 00$ 00

$f_k(L, R) = L \oplus f(R, SK), R$

$= 1001 \oplus$

Permutation P4

0 0 0 0

$f_k(L, R) = L \oplus f(R, SK), R$

$= 1001 \oplus 0000, 1100$

$= 10011100$

1 2 3 4 5 6 7 8

Step-5 IP^{-1}

4 1 3 5 7 2 8 6

1 1 0 1 0 0 0 1

plaintext = 01110010
ciphertext = 11010001